جامعة نايف العربية للعلوم الأمنية

Naif Arab University For Security Sciences

الجرائم المستحدثة والبحث العلمي

"جرائم الحاسب الآلي"

د. محمد سامي السيد الشوا

٢٠٠١م

الجرائم المستحدثة والبحث العلمي
«جرائم الحاسب الآلي»

د. محمد سامي السيد الشوا

الجرائم المستحدثة والبحث العلمي
«جرائم الحاسب الآلي»

المقدمـــــة

إذا كان القرن التاسع عشر قد حصر جل اهتمامه في تنمية مصادر الطاقة، فإن القرن العشرين - ولا سيما النصف الثاني منه سيبقى دوما بالنسبة لتاريخ الاقتصاد قرن المعلومات، ولاشك أن استحداث أجهزة تسمح بمعالجة هذه المعلومات، وهو ركيزة هذه الثورة الهائلة.

ويؤدي الحاسب الآلي والمعالجة الآلية للمعلومات خدمات عظيمة للبحث العلمي والطبي، حيث يتيح لكل منهما تنظيم عمل المنشآت والإدارات بأسلوب علمي.

ولا يستطيع أحد أن يمارس في المزايا والفوائد الخاصة بتقنية المعالجة الآلية للمعلومات، حيث غزا الحاسب الآلي جميع قطاعات ومجالات أنشطة الإنسان، وهذا ما عبر عنه توفيق بقوله «لقد ترك الحاسب الآلي بصمات واضحة على حياتنا الحديثة، وإليه يرجع الفضل في تطوير عدد كبير من أنشطتنا اليومية سواء من حيث المضمون أو الشكل أو الزمن أو المسافة.

ولكن هذا الاستخدام المتزايد لأساليب المعالجة الآلية للمعلومات ليس له دائما، آثار إيجابية، حيث يشاهد في الواقع وبمعدل مطرد، العديد من أوجه الاستغلال المتعسف، وأفعال الاستخدام المقترنة بسوء نية لأداة المعالجة الآلية للمعلومات.

ويعد الإجرام المعلوماتي أحد الأوجه العديدة للتعدي المؤثر على هذه

التقنية في مجال الأعمال والإدارة، وليس المقصود به مشكلة نظرية بحتة في مجتمع مستقبلي تحكمه نظم المعلومات، بل إن الإجرام المعلوماتي هو حقيقة اجتماعية مادية تشغل ذهن كثير من الفقهاء.

وترجع الإرهاصات الأولى لظاهرة الغش المعلوماتي - والتي أصبحت محلاً لأبحاث أكثر تفصيلاً في الآونة الأخيرة - إلى الستينيات عندما طرحت الصحف والكتب العلمية «إجرام تقنية المعلومات» وتعالج هذه البيانات في غالبيتها، التلاعب بالحاسب الآلي وتعطيله والتجسس عليه والاستعمال غير المشروع له. ونظراً لأن الكثير من هذه البيانات قد شيدت بصفة خاصة على تقارير الصحف فكان من العسير جداً، معرفة ما إذا كانت الظاهرة المستحدثة للغش المعلوماتي تعد من قبيل الحقيقة أم الخيال.

ويلاحظ من مراقبة الأبحاث والدراسات التي أجريت في هذا الشأن، عدم اتفاقها على مصطلح معين للدلالة على هذه الظاهرة الإجرامية المستحدثة، فهناك من يطلق عليها ظاهرة «الغش المعلوماتي» أو الجريمة المعلوماتية» أو «الاختلاس المعلوماتي» ويبدو في الحقيقة أنه من الصعوبة بمكان وضع تعريف لظاهرة إجرامية مستحدثة خشية من حصرها في مجال ضيق يمكن أن يضر بها.

ولكن يصبح بالضرورة أن نضع تعريفاً يشمل العناصر الأساسية التي تسمح بتحديد الظاهرة محل الدراسة بهدف التعرف عليها، ويمكن أن نعرف الغش المعلوماتي - وفقا لرأينا - بأنه «كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية نظم المعلومات، ويهدف إلى الاعتداء على الأموال المادية أو المعنوية»، ويسمح لنا هذا التعريف باستبعاد كل الأفعال الإجرامية التي ترتكب بمناسبة الاستخدام العارض للحاسب الآلي

الغش المعلوماتي كظاهرة إجرامية مستحدثة

تمهيد وتقسيم

لا شك أن الحاسب الآلي أصبح على مدى العقدين الماضيين ركيزة أساسية لأهداف التطور في كل مجالات الحياة، بما فيها من أنشطة مختلفة سواء اقتصادية أو علمية أو اجتماعية أو صناعية أو زراعية.

وأدى الاستخدام المطرد للمعلوماتية سواء في شكل «أموال معلوماتية» أو «أساليب مستحدثة» إلى ظهور ما يعرف بالإجرام المعلوماتي، وهذه نتيجة حتمية لكل تقدم تقني مستحدث، ويرتكز هذا النوع من الإجرام على محورين أحدهما ضد المال والآخر ضد الأشخاص. ويستمد نشاطه من الإمكانيات الهائلة للحاسب الآلي[1]

فالحاسب الآلي - كأداة للتخزين - لديه قدرة هائلة على تخزين وتنظيم واستغلال عدد غير محدود من المعلومات، ولديه القدرة أيضاً على استرجاعها في فترة زمنية وجيزة، وقد تكون هذه المعلومات إسمية، وهنا يبرز شبح القضاء على الحياة الخاصة.

والحاسب الآلي - كأداة للادارة - يمكن أن يستخدم في الخير أو في الشر، من أجل زيادة الاستثمار أو لأجل إخفاء الغش.

والحاسب الآلي - كأداة للسلطة - يمكن أن يكون محلا للمعارضة الأيديولوجية والتي تعبر عن نفسها بأسلوب العنف.

---

(١) راجع: M. Masse, Op. cit, P.21,22.

ويبدو أن القوانين العقابية التقليدية عاجزة عن احتواء هذه الظاهرة الإجرامية المستحدثة، وهذا ما أشار إليه الأستاذ Huet حين قرر «أن الجرائم التقليدية والتي صيغت بعد تأمل في الثروات أو في المستندات المعرضة للتلف المادي، تضمن بصعوبة حماية هذه القيم المعنوية الناشئة عن المعلوماتية»[1]، وما عبر عنه الأستاذ Pradel في ختام توصيات مؤتمر المعلوماتية والقانون «يشاهد في ظل المعلوماتية عملية تطويق للسلوكيات المادية»[2]

ولهذا السبب يبدو من المناسب أن نتناول دراسة خصائص هذه الظاهرة الإجرامية المستحدثة، كي توضع في الاعتبار عند تقرير أي سياسة عقابية لها.

وترتيبا على ما تقدم تقسم دراستنا في هذا الباب على النحو التالي:

الفصل الأول: المجرم المعلوماتي.

الفصل الثاني: المجني عليه في الجريمة المعلوماتية.

الفصل الثالث: التقنيات المستخدمة في الجريمة المعلوماتية.

الفصل الأول: المجرم المعلوماتي

ينظر إلى عملية المعالجة الآلية للمعلومات بوصفها محصلة تعاون وعمل مجموعة، والذي يدعمه في كل لحظة أفكار مستحدثة وإبداع، ولكن

(1) J. Huet, La modification du droit, sous l'influence de l'informatique, A spects de droit prive, J. C. P. 1983, 1-3095.

(2) J. Prade, Conclusion du colloque sur l'informatique et Droit penal, Paris Cujas, 1983, p. 155.

هذه العملية محفوفة بمخاطر فقد المعلومات والإفشاء غير المسموح والاعتداء على سلامة النظام المعلوماتي.

ومن المؤكد، وعلاوة على الأحداث الطبيعية التي تهدد حياة والتطبيقات المختلفة للمعلوماتية «كالزلازل والحرائق والفيضانات»، فإن هناك الأحداث التي تنشأ عن عمد وتكون من صنع الإنسان ذاته، وقد تصدر هذه الأخيرة عن إنسان حسن النية وخير مثال على ذلك الخطأ. ولكن الذي يعنينا منها تلك الأحداث الصادرة عن أشخاص من ذوي النوايا السيئة الذين يقترفون أفعال الإتلاف الغش.

وينظر إلى المعلوماتية دائماً بوصفها أداة محايدة وأن مصدر ضعفها وانتهاكها هو الإنسان ذاته، والذي غالباً ما يهيىء فرصة استغلال الوسيلة المعلوماتية، والتي أعدها سواء عن حسن أو سوء نية، ويرتبط جوهر المشكلة إذن بالإنسان وشخصيته ودوافعه[1]

وعلى هدى الدراسات التي تجرى في مجال الإجرام المعلوماتي سوف نبين أولاً خصائص شخصية المجرم المعلوماتي ثم نوضح أنماطه وأخيراً نحلل الأسباب والعوامل التي تدفعه لاقتراف الجريمة المعلوماتية.

---

(١) نشرت شركة IBM للحاسبات الآلية إعلاناً خاصاً بسلامة وتأمين نظم المعلومات، والذي ظهر في العديد من الجرائد الأمريكية ذات الشهرة الواسعة وهو عبارة عن صورة كاريكاتيرية لأربعة من رجال الشرطة وهم يقبضون على حاسب آلي. وجاءتعليقاً على هذه الصورة «أن الحاسب الآلي ليس مدانا»، واستطرد الإعلان قائلاً إن الحاسبات الآلية ليس بإمكانها أن ترتكب بذاتها الجرائم، ولكن يمكن أن تستخدم كوسيلة لارتكابها، راجع في ذلك Parker, op. cit , P.4.

المبحث الأول: خصائص شخصية المجرم المعلوماتي

لا يمكن لأي عقوبة أن تحقق هدفها سواء في مجال الردع العام أو الردع الخاص مالم نضع في الاعتبار شخصية المجرم والذي ينبغي إعادة تأهيله اجتماعيا حتى يعود مرة أخرى مواطنا صالحا لحظيرة المجتمع.

ونبادر بالقول بأن المجرم المعلوماتي يمثل بالنسبة للمجموعات التقليدية للإجرام شخصية مستقلة قائمة بذاتها، فهو من جهة مثال منفرد «للمجرم الذكي» وهو من جهة أخرى «إنسان اجتماعي بطبيعته».

المطلب الأول: المجرم المعلوماتي «كإنسان ذكي»

يقال عادة أن الإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف

وإذا كان من السهل تصور الإجرام العنيف الموجه ضد النظام المعلوماتي والذي يبدو في إتلاف الحاسب الآلي أو الدعائم الممغنطة، والذي يحدث أحيانا في اطار الأفعال الإرهابية.

إلا أنه لا يجب استنتاج أن الإتلاف المعلوماتي بحاجة الى سلوك عنيف، فهو ينشأ من تقنيات التدمير الناعمة، التي تتمثل في التلاعب بالمعلومات أو الكيانات المنطقية أو البيانات.

ويحدث هذا التلاعب عن طريق ما يعرف «بالقنابل المنطقية»، والتي بمقتضاها يتم زرع تعليمات في برنامج مزود بعداد، والذي عندما يصل الى بداية معينة تنطلق هذه التعليمات لكي تمحو البرنامج أو البطاقات، ويتم استخدام هذه الوسيلة من قبل العاملين في المنشآت المعلوماتية بغرض حماية أنفسهم ضد خطر الفصل. وهناك وسيلة أخرى «بديلة» تتمثل في استفهام

البرنامج كل يوم من اسم شخصية المنتفع باستخدامه والمدون في بطاقته الشخصية، فإذا لم يظهر على الاطلاق يصدر أمر باتلاف البطاقات.

وهناك أيضا ما يعرف «بالفيروسات المعلوماتية»، وهي عبارة عن برنامج من الحجم الصغير الذي يصعب اكتشافه ويوضع في اسطوانة، ثم يقوم بنسخ نفسه في نظام تشغيل الحاسبات الآلية وينتشر بعد ذلك في كل الدعائم الممغنطة والمستخدمة في هذه الأجهزة، ويستطيع الفيروس في فترة زمنية وجيزة أن يحطم جميع البطاقات.

ولا يجوز أن يطلق على ممارسة أفعال الإتلاف باستخدام الأساليب التقليدية مصطلح «الغش المعلوماتي» لأنه لكي ينشأ هذا النوع من الإجرام، فإنه يلزم استخدام تقنية خاصة تتعامل مباشرة مع البرنامج أو البيانات.

المطلب الثاني: المجرم المعلوماتي «كإنسان اجتماعي»

نستطيع أن نقرر باستثناء تقنيات المعلوماتية واستخدامها من قبل اللصوص. بأن الإجرام المعلوماتي قد أثمر عن عوامل مستحدثة في أذهان مرتكبيه، حيث يلجأ العديد منهم إلى ارتكاب هذه الجرائم بدافع اللهو أو لمجرد إظهار تفوقهم على الآلة أو على البرامج المخصصة لأمن النظم المعلوماتية، ومن المألوف جداً من جهة أخرى ألا يحصلوا على منفعة مالية من جرائمهم، ولكنهم يكتفون بالتفاخر بأنفسهم وأن يظهروا لضحاياهم ضعف أنظمتهم[1]

---

(1) Yves Bismuth, Criminalite informatique a la reacherche d'une harmonisation legislative, Tpologie et incriminations , Expertises 1988 No, lll, P .376.

وهكذا يشاع في بعض المنشآت التي يضبط بها أحد قراصنة المعلومات بأنه يسعى إلى الحاقه بالفريق المعلوماتي المكلف بضمان أمن النظام المعلوماتي فيها.

ويمكن أن نشير في هذا المجال إلى مثال مثير للدهشة مستمد من اعترافات منهم يبلغ من العمر ١٦ سنة أمام القضاء الجنائي الألماني[1]، حيث نسب إليه ولوجه المقترن بالغش في نظام الفيديوتكس Videotext الخاص بـ Bundespot المعروف بمصطلح «BTX» ودافع المتهم عن نفسه قائلاً «تملكني إحساساً قوى بأن أكون مفيداً في كشف عيوب نظام BTX، ولذا أرسلت في الحال إلى مجموعة عمل أكل العناصر التي اكتشفها بالصدفة والتي أظهرت تشككها فيما يخص حماية البيانات، لا سيما وأن غالبية ملاحظاتي لم تكن معروفة بعد لدى هؤلاء، مما أتاح الأمر إلى تلاشي هذه العيوب».

«ومن جهة أخرى إذا كنت مولعا بنظام BTX، وأكرس نفسي له صباحا ومساء، لكنني لست شريراً على الإطلاق كبعض الأشخاص القائمين على نظام BTX ولا يملكون أي كفاءة».

ولكن لا يجب أن نستخلص من ذلك، إنعدام أي خطر اجتماعي للإجرام المعلوماتي. وليس السبب في ذلك عدم وجود نوايا آثمة، ولكن أيضا للسلوك غير الواعي الذي يمكن أن يتسبب في أضرار جسيمة حتى ولو لم يكشف عن أي عداء للمجتمع.

---

(1) Yves Bismuth, art, prec, p . 377

المبحث الثاني : الأنماط المختلفة للمجرم المعلوماتي

تشير أبحاث علم الإجرام إلى أنه من الناحية العملية، فإن كل تقنية مستحدثة، ينشأ عنها في أي لحظة، وفي أي مرحلة من مراحل تطورها، الظاهرة الإجرامية الخاصة بها. وينطبق ذلك وبوجه خاص على المعلوماتية نظرا للإمكانات المستحدثة التي تقدمها الآلة الالكترونية، من حيث سهولة وسرعة تنفيذ الأفعال الإجرامية وأيضا إخفاء الأدلة.

ويلاحظ علاوة على ذلك، أن أفعال الغش هذه تتمايز قليلا في مضمونها وتنفيذها ومحو آثارها عن تلك الأفعال الخاصة بالإجرام التقليدي حيث يكتفي نصاب المعلوماتية بلمس لوحة مفاتيح الحاسب الآلي Clavier D'irdubateur والتي تقوم بعمليات الحساب والتحليل وإسقاط حواجز وأساليب الحماية الأكثر خداعا.

ويتعين على الفاعل أن يحوز ثلاثة عناصر[1] كي يتدخل تدخلا غير مشروع في ذاكرة الحاسب الآلي لالتقاط المعلومات المختزنة بها أو لتعديلها أو لإتلافها.

١ ـ أن يحوز بنفسه حاسباً آلياً مصغراً ونهاية طرفية وهي عبارة عن محطة للتراسل بين المستعمل والحاسب الآلي، أو أن يكون لديه على الأقل الشفرة.

٢ ـ أن يكون مزوداً بمودم عبارة عن أداة لترجمة تعليمات مكتوبة بلغة الحاسب الآلي إلى رموز رقمية أو العكس، حيث يسمح للحاسبات الآلية أن تستقبل وتنقل المعلومات عن طريق وسيط لخط تليفوني.

---

(1) J. Said, The . prec. p . 19.

٣ـ أن يكون لديه قدر لا بأس به من الحيل والكفاءة والمواظبة.

وقبل أن نشرع في رسم صورة لمرتكبي أفعال الغش المعلوماتي المحنكين، فإنه يحسن أن نلقي نظرة سريعة على مجموعة خاصة من المخادعين، والذي يطلق عليهم عادة صغار نوابغ المعلوماتية»[1]

المطلب الأول: صغار نوابغ المعلوماتية

ويقصد بهم الشباب البالغ المفتون بالمعلوماتية والحسابات الآلية وكثيرا ما لفتوا النظر في الأزمة الأخيرة عقب أفعال الانتهاك غير المسموح بها في العديد من ذاكرات الحاسبات الآلية. وتقترف هذه الطائفة أفعالها الإجرامية

---

(١) عقدت ندوة حديثة لوكالة البرامج Agence pour la protection des programmes بخصوص جرائم نظم المعلومات، وانتهت إلى تصنيف التقنيات إلى أربع مجموعات:

الأولى: وهي أكثر المجموعات رأفة ويمثلها طبقة من الشباب لديهم قدر لا بأس به من الخبرة المعلوماتية، ويمارس مواهبه في المساء، على الحاسب الآلي Minitel بغرض الولوج في نظم المعلومات لأجل ممارسة هواية اللعب.

الثانية: وهي من نفس نمط المجموعة ولكنها تتفوق عليها علما ومعرفة بعملية البرمجة وغايتها أيضا التسلية والملاحظة.

الثالثة: وهي أكثر المجموعات ضرراً، ولها نفس كفاءة المجموعة ولكنها لاتكتفي بالملاحظة بل تلجأ إلى أفعال الاعتداء العمدي.

الرابعة: وهي أكثر المجموعات خطورة، ولها نفس هدف المجموعة السابقة «أي الإرهاب المعلوماتي» ولكن باستخدام وسائل على قدر كبير من البراءة، كزرع برامج الفيروسات والقنابل المنطقية خلسة والتي ينشأ عنها أضرار جسيمة.

Michel kessler, L'investissement informatique de L'Enreprise et sa protection penale , G. p. 1990 No. 365, p . 6.

عن طريق استخدام حاسبات آلية ميكروية خاصة بهم أو بمدارسهم، ولا يحد أفعال اعتداءاتهم حدود جغرافية حيث تصل اعتداءاتهم على أنظمة ومراكز المعلوماتية إلى عدة آلاف من الكيلومترات من أماكن تواجدهم.

إلا أنه من الأهمية بمكان أن نكون أكثر حذراً بالنسبة لهذه الطائفة من مرتكبي أفعال الغش المعلوماتي. حيث تميل الصحافة «وهي المصدر الخصب لنشر الأفعال» أحيانا وعن عمد إلى التضخيم من هذه الظاهرة، باعتبار أن العناوين الجذابة هي أساس التسويق، وأن غالبية الأفراد عادة ما يكونون مفتونين بهذه الأنشطة الإجرامية المبتكرة والمستحدثة.

ونحن من جانبنا سوف نكتفي بالإشارة إلى الأمثلة التي وردت في تحقيقات أجرتها هيئات رسمية[1] أو جرائد متخصصة[2]

ونذكر هنا على سبيل المثال العصابة التي يطلق عليها «٤١٤» والتي تقطن الولايات المتحدة الأمريكية وقد نسب إليها ارتكاب ستين فعلاً تعد على ذاكرات الحاسب الآلية مما نجم عنها أضرار لحقت بالمنشآت العامة والخاصة.

ولا يبدو لنا من الملائم أن نصنف هؤلاء الشباب البالغ في طائفة أو أخرى من الطوائف الإجرامية لأن لديهم ببساطة ميلاً للمغامرة والتحدي والرغبة في الاكتشاف، ونادرا ما تكون أهداف أفعالهم المحظورة غير شريفة، وهم لا يدركون ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة تجارية.

---

(1) S.R.I.F.B.I.O.C.D.E.C.E.

(2) Compter Fraud, Le Monde Informatique, Expertises.

ويشاهد في الولايات المتحدة وأحيانا في أوربا رد فعل مباشر من السلطات، والذي يتمثل في التحقق من المجرمين مرتكبي أفعال الغش المعلوماتي، ومصادرة أجهزة الحاسبات الآلية الخاصة بهم، وهي أداة الفعل الإجرامي[1]

ونستطيع أن نقرر، بأن هذا النمط من أفعال الغش، والذي يرتكبه هؤلاء الشباب لاخوف منه على الإطلاق.

وعلى النقيض يكشف هذا النمط من أفعال الغش عن قلق مؤكد، وهو يعكس الاهتمام بمشكلة أخرى أكثر تعقيداً، ونعني بها المخاطر التي تطارد الأسرار والمعلومات المحفوظة في الذاكرات الصناعية للحاسبات الآلية، أو تلك التي تنتقل من خلال شبكات Teletransmission

وإذا كان بإمكان هؤلاء الشباب الهاوي انتهاك الأنظمة، على الرغم من حمايتها، إلا أنه يخشى من التدخل الحقيقي لمحترفي أفعال الغش والتجسس أو من ماهري قرصنة المعلومات.

وعلاوة على ذلك، فإن الخطر الذي يواجه هذه الطائفة، يتمثل في احتمال الانزلاق الذي يمكن أن يحدث، من مجرد هاو صغير للأفعال غير المشروعة إلى محترف لأعمال السلب والخطر الثاني الأعظم والذي يتعين مواجهته، يتمثل في احتضان منظمات أو أفراد غير شرفاء لهؤلاء الشباب.

---

(1) D. Parker, op. cit, p. 122 ets.

يكتسب هذا النمط المستحدث من الأفعال غير المشروعة، والمرتبط بالاستخدام التعسفي للحاسب إلى خطورة خاصة، نظرا لتقنيتها العالمية من جهة، ولغموض شخصية مرتكبيها من جهة أخرى.

وتوضح الدراسات التي أجراها معهد Standford Research على سبعمائة جريمة معلوماتية، وأيضا من الدعاوى التي تم تحريكها في هذا الشأن سواء في الولايات المتحدة أو في أوربا أن مرتكبي أفعال الغش المعلوماتي من الجيل الحديث، هم غالبا من الشباب الذين تتراوح أعمارهم من ٢٥ إلى ٤٥ سنة، وهي المرحلة الزمنية التي تتناسب مع تعميم تقنية المعلوماتية[1]

ويتشابه مرتكبو هذه الأفعال الآثمة مع المجرمين ذوي الياقات البيضاء من حيث كونهم من أصحاب التخصصات العالية، ولهم الهيمنة الكاملة على تقنية الالكترونيات، وعلى قدر من الذكاء.

وتشهد الإحصائيات التي أجريت في هذا الشأن على كفاءة محترفي أفعال الغش المعلوماتي[2]

- حيث يأتي في المقدمة المحلل information والذي يقترف نسبة تقدر بحوالي ٢٥٪ من أفعال الغش.
- ثم المبرمج والذي يرتكب حوالي ١٨٪ من أفعال الغش.
- ثم المستخدم الذي لديه أفكار معلوماتية تتجاوز الولوج في النهايات الطرفية بنسبة تقدر بحوالي ١٧٪.

---

(1) Co.pit. I.J.Said, The prec., . 23.

ـ ثم الصراف بنسبة تقدر بحوالي ١٦٪.
ـ ثم الشخص الأجنبي عن المنشأة بنسبة تقدر بحوالي ١٢٪.
ـ وأخيراً المشغل Operateur بنسبة تقدر بحوالي ١١٪.

وفي الحقيقة، فإنه يبدو من الصعوبة تصور ما إذا كنا في مواجهة مجرمين حقيقيين، وذلك بالنسبة لجزء من هؤلاء مرتكبي أفعال الغش، ويبدي مرتكبو أفعال الغش المعلوماتي ـ في المرحلة الأولى من تكوينهم ـ نشاطاً ملحوظاً.

وكثيراً ما ينظر إليهم بوصفهم مستخدمين مثاليين، ويشغل الغالبية العظمى منهم مراكز قيادية، ويتمتعون علاوة على ذلك بثقة كبيرة في مجال عملهم وكثيراً ما يقومون بتغيير وظائفهم أثناء نشاطهم الحرفي[1]

وهذه السمات الخاصة، هي التي تصنع هؤلاء مرتكبي أفعال الغش المعلوماتي، وهي تتطابق كثيرا مع التقنية التي يستعملونها أكثر من تطابقها ومصالح المنشآت التي يعملون بها.

وقد قام فريق من علماء النفس، بدراسة عدد من شخصيات مرتكبي أفعال الغش المعلوماتي. ولاحظوا أن هؤلاء المخادعين لا يعيرون أدنى اهتمام إزاء القيم التي ليست لها آثار مادية ولا يدركون دائماً أن سلوكهم يستحق العقاب[2]

---

(1) Co.pit, I.J.Tappolet, La fraude informatique Rev. int. crim. pol. tech. 1988, p . 351.
(2) Droit penal de l'ionformatique , in Documents publies par I.B.I.No. 7 janv. 1983, p . 3.

ونستطيع أن نقرر بأن الاستخدام المتزايد للحاسبات الآلية قد أنشأ مناخاً نفسياً موائماً لتصور مضمونه استبعاد «فكرة الخير والشر» وقد ساعد ذلك على عدم وجود احتكاك مباشر مع الأشخاص. والذي تملك حيالهم الإحساس بسلب «الخبز من الفم» وأن هذا التمزق في العلاقة الثنائية «بين الفاعل والمجني عليه» يهدىء الوسوسة المحتملة، ويسهل فيما يبدو المرور إلى الفعل غير المشروع، ويشجع هكذا على إيجاد نوع من الإقرار الشرعي الذاتي.

ويبقى مع ذلك، ألا نسبح في الخيال، حيث لا يمكن أن ننكر أنه من بين الحالات التي خضعت للبحث، وجد عدد من مرتكبي أفعال الغش المعلوماتي لديه اتجاه إجرامي خطير، ويبرز ذلك على وجه الخصوص في بعض الأعمال التي لها طابع المنافسة الشرسة والتي تستعمل المجرمين المحنكين وأيضاً في أعمال التجسس.

وينبغي الإشارة إلى أن في الغالبية العظمى من الحالات المكتشفة لأفعال الغش المعلوماتي، قد ارتكبت بواسطة مستخدم من المنشأة التي تدار بنظام المعلوماتية، أو على الأقل عن طريق اشتراكه فيها، حيث يعد ذلك أمراً ضرورياً وحتمياً.

أولاً: الفاعل في جريمة الغش المعلوماتي

كثيرا ما يلجأ المستخدمون العاملون بمنشأة تداربالنظام المعلوماتي إلى ارتكاب أفعال الغش المعلوماتي التي تستهدف الحاسبات الآلية وهم ينفذون هذه الأفعال أما لحسابهم أو لحساب أشخاص أجانب مقابل دفع مبلغ من المال.

وهناك حالة ارتكب فيها فعل «الغش المعلوماتي» بواسطة مستخدمي المنشأة ولحسابها أيضاً بموافقة واشتراك إدارتها[1]

وهذا ما حدث بإحدى شركات التأمين بمدينة لوس أنجلوس الأمريكية حيث تمكن مستخدموها وبمساعدة نظامها المعلوماتي. من خلق عملاء وهميين مؤمن عليهم، وقد تمكنت هذه الشركة من بيع ٤٦. بوليصة تأمين إلى شركات مناظرة في إطار اتفاقيات تثنية التأمين[2]

ويوضح هذا المثال أن نظام المعلوماتية هو ألعوبة هؤلاء القائمين على تشغيله ومراقبته، أي المحللين أنفسهم.

فهم يملكون المعرفة اللازمة والتقنية الكافية للتلاعب بالحاسبات الآلية وفقا لهواهم، وهم يشكلون من أجل ذلك الخطر الأعظم الكامن.

ويبدو إذن أن أكثر الأنظمة المعلوماتية أداء وخداعاً، تعد عرضة أيضا للانتهاك والتعدي، ويصبح سلوك مرتكبي أفعال الغش المعلوماتي في مأمن من عدم العقاب، حيث يستخدم منتهكو القوانين الامكانيات والأساليب المعلوماتية ليس فقط من أجل ارتكاب فعل الغش. بل وللتهرب من كشف أمرهم أو على الأقل إعاقة الملاحقة القضائية لهم لعدم وجود أدلة، وعلاوة على ذلك، فالاشتراك أو المساعدة، غالبا ما تكون ضرورية من أجل الاقتراف المحترف لأفعال الغش المعلوماتي[3]

---

(1) J. Said, The prec. p. 24.

(2) Fraude a l'Equity Funding life insurance, Dans i'Informatique Nouvelle Mai 1976, no 73.

(3) L'article de J. M.Chabans, in le Monde Dumache du 6 janv. 1980.

ثانياً : الشريك في جريمة الغش المعلوماتي

يتميز الغش المعلوماتي بحقيقة مؤداها : أن دقة وتنفيذ العمليات غير المشروعة، يستلزم مشاركة أو مساعدة أشخاص آخرون «سواء أكانوا فنيين أو مجرد وسطاء». وقد يكون هذا الاشتراك سلبيا، والذي يترجم بالصمت وذرهم يفعلون، ولكن غالباً ما يكون إيجابياً، ويتمثل في مساعدة فنية أو مادية.

وتستلزم آليات الابتكار لمخادعة الحاسب الآلي - الاستعانة بمجموعة من الوسطاء، أي شركاء مؤتمنين على أسرار اسطوانات الحاسبات الآلية، وهؤلاء هم الدعامة الأساسية لنجاح العملية غير المشروعة والمستهدفة.

ومن جهة أخرى، قد تبدو المساهمة الفنية أمرا حتميا بالنسبة لهؤلاء المجرمين الذين لا تتوافر لديهم هذه الكفاءة الفنية والتي تؤهلهم للتلاعب بالحاسب الآلي وفقاً لهواهم.

وفي النهاية وطالما أننا بصدد مساعدة متبادلة بين مرتكبي أفعال الغش المعلوماتي - فإنه يمكن الحديث عن «التزامن التباني للاشتراك[1] وهو الذي يسمح بالتحريض التبادلي تجاه تنمية الميل إلى الأعمال الباهرة والمآثر، وفي النهاية إلى دقة متناهية في أساليب وتقنيات اقتراف أفعال الغش المعلوماتي.

ويمكن التساؤل بعد دراسة شخصية مرتكبي الجرائم المعلوماتية عن ماهية الأسباب الرئيسية التي تحرض هؤلاء على اقتراف أفعالهم غير المشروعة ؟

---

(1) Droit penal de L'informatique, Document I.B.U. No. 7, Janv, 1983.

المبحث الثالث : الأسباب الرئيسية للجريمة المعلوماتية

وكما سبق الإشارة، فإن أنماط مرتكبي أفعال الغش المعلوماتي، تختلف قليلاً عن مرتكبي الأفعال الإجرامية التقليدية، ومن ثم فليس من المستغرب أن نجد الاختلف في الأسباب والعوامل التي تدفع إلى اقتراف الفعل غير المشروع.

وبالتأكيد، فإن أمل الربح وروح الكسب هي التي تدفع إلى ذلك دائماً، ولكن وسائل بلوغ هذا الهدف هي التي تتغير، حيث تتمثل هنا في استخدام الحاسبات الآلية والإمكانيات المستحدثة للمعلوماتية.

وعلاوة على ذلك، تبين من فحص عدد كبير من أفعال الغش، أن شخصية المجرم المعلوماتي تتسم بالنشاط والمخاطرة والذهن المتقد الذي يسعى إلى خداع الآلة.

وفي كل مرة يتحقق فيها الاخفاق وفقا لمنطق النظام المعلوماتي، فإنه لا يمكن سوى ملاحظة أن الإبداع اللانهائي لأفعال الغش البارع يستمر ويتطور بمعدل يفوق أساليب الحماية والجزاء المطبق.

وفي النهاية، يمكن القول بأن الشغف بالآلة الإلكترونية، والانجاز التقني، والرغبة في الكسب، هي الأسباب المحرضة التي تدفع بعض مستخدمي الحاسبات الالية إلى استغلالها على نحو غير مشروع.

طالعتنا مجلة Expertises الفرنسية في سبتمبر ١٩٨٣م بقصة عنوانها «ميلاد نزعة»[1] وتتلخص أحداثها في توجه عامل طلاء مباني إلى أحد البنوك لإيداع شيك خاص به، وتعاصر ذلك ولحظة فصل الموزع الآلي للنقود حيث شاهد مستخدم صيانة الأجهزة الآلية، وهو يقوم باستخراج نقود البنك من الآلة «عند الطلب»، عن طريق استخدام بطاقة خاصة

وقد أحدث هذا الابتكار للآلة، تصدعا في الحياة العادية لعامل الطلاء والذي يدعى Roland Lave وقد حرص هذا الأخير على التدريب على تقنية الحاسب الآلي لمدة عامين، ثم قام بالسطو على صانع الموزعات الآلية، وقد تمكن Roland بفضل الآلة المسروقة من التوصل إلى أسلوب مطالعة السحب Cartes de retrit وقد ألقي القبض عليه قبل أن يستفيد من نزعتها المستحدثة، وقد نسب إلى جريمة سرقة الآلة.

ويجب أن نقرر علاوة على ذلك أن هناك العديد من الأمثلة وحالات العجز التقني التي تترك الفرصة لمشيدي برامج الحاسب الآلي لاقتراف أفعال الغش المعلوماتي.

ودائما ما يوضع في الاعتبار دقة الأسلوب أكثر من فعل الغش ذاته، ويميل مرتكبو أفعال الغش المعلوماتي إلى إظهار تفوقهم ومستوى إرتفاء براعتهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة، فإن مرتكبي أفعال الغش الذين لديهم شغف بالآلة، يحاولون إيجاد «وغالباً ما يجدون» الوسيلة إلى تحطيمها.

---

(1) Naissance d'une vocation Expertises, No. 42 Fev. 1983.

والجدير بالملاحظة أن بعض مرتكبي أفعال الغش المعلوماتي ليسوا على جانب كبير من الخطورة الإجرامية، وهم يكتفون في العادة بتحقيق انتصارات تقنية، ودون أن تكون لهم نوايا آثمة.

وهناك بواعث أخرى، غالبا ما تكون آثمة وغير شريفة، تحض على ارتكاب أفعال الغش المعلوماتي، وهي على قدر كبير من الخطورة بالنسبة لسير أو انتظام المنشأة أو النظام المشتبه فيه.

المطلب الثاني: السعي إلى الربح

الرغبة في تحقيق الثراء الشخصي. هي الدافع إلى الغش الأكثر انتشارا ويبدو ذلك جلياً من خلال تحقيق أجرته إحدى المجلات المتخصصة بخصوص موضوع «الأمن المعلوماتي»[1]، ومن خلال ماذكره الأستاذ Parker[2]:

- ٤٣٪ من حالات الغش المعلن عنها، قد بوشرت من أجل اختلاس الأموال.
- من أجل سرقة معلومات.
- ١٩٪ أفعال إتلاف
- ١٥٪ سرقة وقت الآلة Vol de temps machine «أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية».

وفي الواقع، فإن المحرك لاقتراف فعل الغش المعلوماتي. يمكن أن ينطلق من مجرد النجاة من غرق الديون المستحقة، أو من المشاكل العائلية

(1) G. Delmare, Securite informatique, Ressource informatique no. 1, Juill, 1984.
(2) D. Parker, Op. cit, p. 120 et s.

الراجعة إلى النقود، أو من الخسائر الضخمة لألعاب القمار، أو من إدمان المخدرات، وقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه المرحلة، فالغاية تبرر الوسيلة. ولذا فإن بيع المعلومات المختلسة هو نشاط متسع للغاية. ويمكن أن نذكر في هذا الشأن واقعة استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على اثنين وعشرين شريطا تحوي معلومات هامة بخصوص عملاء وانتاج الشركة. وقد هدد السارق ببيعها للشركات المنافسة مالم تدفع له فدية مقدارها ٢ دولار

وقد قامت الشركة بتحليل الموقف، وفضلت دفع المبلغ من أجل استرداد الشرائط الممغنطة المسروقة، حيث قدرت أن الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثير المبلغ المطلوب.

وهناك مثال آخر خاص بمجموعة من رجال شرطة دالاس الأمريكية، حيث تمكنوا بواسطة التلاعب في برنامج الحاسب الآلي الموجود في حوزتهم والمختزن فيه محاضر الشرطة، من إسقاط بعض الغرامات المستحقة مقابل مبلغ من المال[1]

وقد دفعت الرغبة بمستخدم يعمل لدى إحدى شركات التأمين كي يحتفظ بوظيفته التي سبق أن فصل منها، إلى أن يحتجز كرهينة الذاكرة المركزية للحاسب الآلي الخاص بالشركة

وقد هدد المختلس رئيسه في العمل، بأنه إذا حاول أن يلغي بطاقة أجرته من ذاكرة الحاسب الآلي، فإن هذه الأخيرة سوف تدمر تلقائياً عن طريق ما يعرف بالقنبلة المنطقية[2]

---

(1) Le Monde inormatique , 21 fev. 1983, Etude: La delinquance en col blanc se part bien.

(2) La Monde informatique 21 fev. 1983.

ويمكننا أن نلاحظ، ومن ثم أن نستنتج من مجرد حصر أفعال الغش المعلوماتي. أن الأمل في تحقيق الربح هو السبب الأساسي الذي يسيطر على هذه الأفعال. ونستطيع أن نقرر أيضاً احتفاظ البنوك وشركات التأمين بقائمة من أفعال التعدي والتي ليست لها في ذاتها قيمة معتبرة سوى تقوية ومعالجة أنظمتها المعلوماتية[1]

المطلب الثالث: الدوافع الشخصية والمؤثرات الخارجية

الإنسان - حتماً - مخلوق هش من الناحية السيكولوجية حيث يمكن في بعض المواقف أن يستسلم للمؤثرات الخارجية، أو أن يكون قد فرض عليه سلوكه المخادع بدافع من الإكراه أو الحقد.

وقد دفع الانتقام في هذا الخصوص بمحاسب شاب، إلى أن يتلاعب بالبرامج المعلوماتية، وبحيث بعد مضي عدة أشهر من رحيله من المنشأة التي يعمل بها، تختفي كل البيانات الحسابية الخاصة بديون هذه المنشأة، وقد تحقق المحتوم - كما هو موقع - في التاريخ المحدد[2]

وإذا نظرنا من جهة أخرى إلى الحاسب الآلي بوصفه أداة سلطة فهو محل اعتراضات أيديولوجية، يمكن أن تتبلور في صورة أفعال تعد وتدمير لأنظمة المعلوماتية.

وقد أمكن الكشف في بعض المواقف الأخرى، عن أن مجرد إظهار شعور جنون العظمة، هو الدافع لارتكاب فعل الغش المعلوماتي، وفي

---

(1) Les escrocsa l'informatique in le Nouvel Economiste no. 202 du 1, 10-1979.

(2) Comment se proteger contre le crime informatique, Temps reels, 26-4-1984.

هذا الشأن نجد المحلل أو المبرمج المعلوماتي . وهو مفتاح سر كل نظام . وقد ينتابه إحساس بالإهمال أو النقص داخل المنشأة التي يعمل بها . وقد يندفع تحت تأثير رغبة قوية من أجل تأكيد قدراته التقنية لإدارة المنشأة إلى إرتكاب فعل الغش المعلوماتي ، وقد يعترف به ، ومن ثم يجد ترضية من خلال الإفصاح عن شخصيته أمام العامة .

وتمارس أفعال الغش المعلوماتي - والتي تنفذ تحت تأثير أو ضغط من الغير - في بعض مجالات الأعمال التجارية وعلى وجه الخصوص في نطاق المنافسة والتجسس[1]

وقد تدفع الحاجة إلى توفير سنوات عديدة من البحث وتجنبا لاستثمار الملايين من الجنيهات التي تتكلفها عملية البحث العلمي ، نقول تدفع هذه الحاجة بعض المنشآت بل بعض الدول ، إلى الاتصال بالأفراد الذين يشغلون مراكز مرموقة كي يعملوا لصالح منشآت أخرى منافسة بهدف الإطلاع على بعض المعلومات الأساسية وتستخدم أساليب عديدة للوصول إلى الهدف المنشود أو المعلومات المشتهى فيها ، وأكثرها شيوعا الرشوة ، الإغراء ، الخداع ، وعند اللزوم الاقناع المقترن بالإكراه أو التهديد بإفشاء نقاط الضعف لدى الفرد المعني .

ولا يكتفي في بعض المجالات ، والتي تبدو على قدر كبير من الحساسية ، بمجرد الاتصال ، بل يفضلون زرع جواسيس خاصة بهم . ونذكر في هذا الخصوص واقعة موظف يعمل بأحد مكاتب شركة مشهورة متعددة الجنسيات ومركزها مدينة Sindelginden بألمانيا الغربية «قبل توحيدها» حيث

---

(1) Tidemann, art prec. p . 616.

كان يتمتع هذا الموظف بسمعة طيبة لدى كل المنشآت العميلة، وقد لوحظ عقب اختفائه، أن هذا الموظف المثالي كان يعمل في الحقيقة في مجموعة جواسيس أنشئت خصيصا في ألمانيا الغربية من أجل مهاجمة أنظمتها المعلوماتية، وقد نجح هذا الجاسوس في أن ينقل إلى ألمانيا الشرقية معلومات هامة بخصوص ٨,٠٠٠ منشأة تعمل في ألمانيا الغربية، ولكن يجب الاعتراف بأن هذا الجاسوس كان ضحية لعملية ابتزاز[1]

المطلب الرابع: أسباب خاصة بالمنشأة

لا شك أن الشخص المسئول عن المركز المعلوماتي، هو بدون منازع في وضع يمكنه من استغلال - إذا ما شاء ولمصلحته - نقاط الضعف المحتملة لمركز المعالجة Centre de traitement وتعد الألفة المتبادلة بينه وبين الأنشطة التي يزاولها ومركز الثقة الذي يحوزه أفضل أسلحة له لارتكاب أفعال الغش المعلوماتي.

ولا يجب أن نغض الطرف، عن أن أحد التهديدات العظمى التي تؤثر على الأنظمة المعلوماتية، هو أن يعهد بكل مسئولية المركز إلى شخص واحد بمفرده، فقد تدفع هذه الثقة العمياء لمحللي ومبرمجي الحاسب الآلية، إلى استخدام النظام لمصلحتهم الخاصة. ونذكر في هذا الشأن أحد أفعال الغش المعلوماتي الأكثر ربحاً، والذي اقترف عن طريق الاستخدام غير المشروع للحاسب الآلي[2] وتتلخص وقائعه في أن مستشارا لدى أحد البنوك الكبرى ويدعى Stanley Rifkin، وكان يتمتع بثقة مطلقة من جانب هذا

---

(1) J. Said. The prec , p . 35 .

(2) L'informatiqu Enou Velle, sepl980, p. 20, Temps reels no. 7, 9-2-1981 .

البنك . وقد سمحت اخصاصاته بالولوج في مفتاحين الكترونيين من ثلاثة أساسية للتحكم في التحويلات الالكترونية للنقود من بنك الى بنك آخر وقد تمكن بفضل قدراته في مجال المعالجة الآلية للمعلومات وتآلفها الشديد مع النظام المعلوماتي من الوصول الى المفتاح الثالث ، واستطاع أن ينقل في الحال ١٠ ملايين دولار الى حساب بنكي فتح باسمه في سويسرا ، وقد ألقي القبض عليه ، صدر ضده حكم بالسجن لمدة ست سنوات .

وهناك جانب آخر من المسئولين عن الأنظمة المعلوماتية ، استفادوا من مواقف خاصة وأحداث جديدة من أجل ارتكاب أفعالهم الآثمة : كحالة رعب في مركز المعالجة ، أو الذعر المصطنع أو إحتجاز المعاملات عن طريق إحداث إشباع أو مجرد استغلال أزمة في المنشأة «كتغيير الإدارة على سبيل المثال» .

لكن على كل حال ، يجب ألا نغض الطرف ، عن أن التسامح والتساهل الذي يهيمن دائماً على تطبيق إجراءات المراقبة وممارسة التفتيش ، يعد من العوامل التي تساعد على تضخم أفعال الغش المعلوماتي .

وفي النهاية فإن الهدف الأساسي من دراستنا التي خصصناها للتعرف على شخصية مرتكبي أفعال الغش المعلوماتي الذين ينتمون إلى الجيل الجديد هو الاقتناع بأن أفضل حماية ، تبدأ دائماً بالمعرفة الجيدة والكاملة للعدو المنتظر

الفصل الثاني: المجني عليه في الجريمة المعلوماتية

وفقا لتقدير بعض خبراء الصندوق الدولي للبنوك F.B.I. فإنه من المستحيل أن تحدد على نحو دقيق نطاق الجرائم المعلوماتية[1]

ولا يعلم ضحايا هذه الجرائم شيئاً عنها، إلا عندما تكون أنظمتهم المعلوماتية هدفا لفعل الغش، وحتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل. فلا يوجد من يريد الاعتراف بانتهاك نظامه المعلوماتي.

وعلى الرغم من ذلك، فقد استطاع اتحاد البنوك في جنيف أن يقدر خسائر أوربا الغربية من ظاهرة الغش المعلوماتي حيث بلغت حوالي ٥٤ مليون فرنك فرنسي عام ١٩٨٨م. كما قدرت خسائر الاقتصاد الأمريكي الناشئة عن هذه الظاهرة بحوالي ٤٠٠ مليون دولار وفقا لما أشار اليه[2]

المبحث الأول: القطاعات المستهدفة

تشير الإحصاءات النادرة في هذا المجال، إلى أنه عملاً، فإن جميع الأنشطة التي تستخدم الحاسب الآلي تكون عرضة لخطر ظاهرة الغش المعلوماتي، فأي قطاع من الأنشطة ليس بمنأى عن ذلك، ويبدو بجلاء أن انتهاك هذه الأنظمة المعلوماتية هو الأكثر توفيرا بالنسبة للمحتالين.

ويلاحظ من ذلك أن الاتجاه الأساسي للغش المعلوماتي. يستهدف البنوك، ووفقا لتحقيق باشرته مجلة Ressources informatiques[3] تبين أن :

---

(1) Y. Bismuth art prec, p. 377.

(2) D. Prker, op. cit. p. 145.

(3) Ressources informatique no. 7, juin-juill, 1984, p. 37.

٩٠٪ من أفعال الغش المعلوماتي تستهدف البنوك

١٦٪ للإدارة.

١٠٪ للإنتاج الصناعي.

١٠٪ للمعلومات

ثم يلي ذلك شركات التأمين والشركات الخاصة.

ويستهدف الغش المعلوماتي في الحقيقة المنشآت المالية، أو على الأقل تلك التي تهيمن على القيم الرأسمالية.

ومن جهة أخرى، فإن المعلومات هي أحد المصالح الأساسية المستهدفة بعد النقود، وأصبحت منذ الآن فصاعدا هي المنفذ الى اقتصاد السوق، وقد شيدت على أساسها صناعة حقيقية ومتطورة.

ولقد نما إلى جوار «السوق الشرعي للمعلومات» «السوق السوداء للمعلومات» وفيه تتم مقايضة وبيع المعلومات المسروقة، أو المقتبسة من أصحابها الحقيقيين والشرعيين[1]. ويرتبط هذا النوع من الإجرام إذن بالجزء الأعظم للأنشطة الاقتصادية والاجتماعية للمجتمع. ويمكن تصوره بالنسبة للمعلومات الآتية :

أ ـ المعلومات المالية

حيث تمس هذه الظاهرة المركز الحسابي والإداري وتنقلات الأموال والاستثمارات سواء في المنشآت العامة أو الخاصة.

---

(1) Said. The prece.p .39.

ب ـ المعلومات التجارية والصناعية

حيث تستهدف هذه الظاهرة الدراسات الخاصة بالأسواق ومشروعات الاستثمار والتصنيع والإنتاج والتجارة والتوزيع والأسعار ومراكز البيع والقطاع الصناعي للإنتاج.

ج ـ المعلومات الشخصية

وهي تلك المختزنة في ذاكرات الحاسبات الآلية للبنوك وشركات التأمين ولدى المحامين والمستشفيات وأقسام الشرطة والأحزاب والنقابات، وقد تهدد هذه الاعتداءات مباشرة قدسية وسرية الحياة الخاصة أو الحرية النقابية والسياسية . الخ.

د ـ المعلومات العسكرية

والتي تتمثل في أسرار الدولة والمشروعات النووية والتصنيع الحديث للأسلحة الخ ويبدو أن هذه المعلومات الأخيرة هي الأكثر رواجا في «سوق المعلومات السوداء».

ويمكن الاستئثار بهذه المعلومات، عن طريق معالجتها معالجة معلوماتية ومؤدى ذلك أن مجرد المعالجة المعلوماتية يسمح بإدارتها على نحو جيد وعلى الرغم من المخاطر التي يمكن أن تتعرض لها هذه الإدارة الآلية، وهذا ما يستلزم احتياطات وتدابير قاسية، ولهذا السبب، يبدو من المفيد معرفة ردود أفعال ضحايا هذه الظاهرة.

المبحث الثاني: ردود أفعال ضحايا الجريمة المعلوماتية

إذا كان عقاب أفعال الغش المعلوماتي ما زال محدوداً جداً إلى الآن،

فمرد ذلك أسباب عديدة : بعضها فني والآخر قانوني والثالث إنساني .

وفي الواقع ، فإن التقنية العالية التي تتسم بها هذه الظاهرة ، هي إحدى العقبات الأساسية في اكتشاف الأفعال غير المشروعة التي تنشأ عنها . وهذا ما يفسر أن جزءاً صغيراً من أفعال الغش هو الذي تم اكتشافه . وعلاوة على ذلك فإن الصدفة[1] وحدها هي التي لعبت دوراً في كشف الغالبية العظمى من الحالات المكتشفة .

وعلاوة على ذلك ، وعلى فرض اكتشاف فعل من أفعال الغش المعلوماتي تثور هنا مشكلة أخرى خاصة بالإثبات المادي لفعل الغش . والمسئولية المحتملة لهؤلاء الذين لهم حق الاشراف على المركز المستهدف ، وهل لهم الصلاحيات اللازمة من أجل تطبيق وتنظيم مراعاة تعليمات الأمن؟ وهل لديهم السلطات اللازمة لإمكان التقدير ووضع التنظيمات الضرورية في حالة حدوث أضرار ناشئة عن إفشاء معلومات على قدر من الحساسية .

ولا يمكن من جهة أخرى تقدير نطاق أفعال الغش المعلوماتي ، وذلك بسبب ردود الأفعال السلبية لضحايا[2] هذه الأفعال ، ويبقى سكوت وسلبية هؤلاء الضحايا خير معين لمرتكبي هذه الأفعال .

---

(1) Vivant et le stanc, in Lany informatique Tiedmann, art prec, p. 613,Jaeger, La fraude informatique , Rev. dr. pen, Crim, 1985, P. 337, Bertinet et de lamberterie . la protection logiciel, ed des parques 1984, p. 337.

(2) Le phenomene de lafraud informatique Analyse de la politique juridique dans la zone de L'O.C.D.E., rapport 1984, p. 24 Tiedmann prec, 613, B. de Schutter, art prec p. 386, pradel et fuillard les infractions commises au moyen de lordinateur, 1985, 320 Rev. dr. pen, crim, 1985, p. 330.

ويميل الغالبية العظمى من هؤلاء الضحايا إلى الحفاظ على سمعتهم التجارية ومكانتهم المرموقة، والقليل منهم هو الذي يكشف عن أفعال الغش التي وقعوا ضحية لها ويعترفون بنتائجها[1]

وغالباً جدا، ما يشغل مرتكبو أفعال الغش المعلوماتي مركز المسئولية ويحتلون مراتب عليا في التدرج الوظيفي بالمنشآت التي يعملون بها، وهذا ما يدفع مديرو هذه المنشآت إلى التستر على المسألة وحل المشكلة في داخل المنشأة.

وهناك حالات عديدة، تمكن فيها مرتكبو أفعال الغش المعلوماتي من تحسين أوضاعهم المالية نتيجة لمهارتهم في اقتراف الأفعال غير المشروعة، وكان قد سبق وعدهم بشغل مراكز هامة في محطة المراقبة أو إدارة الأمن المعلوماتي.

وما يبعث على القلق حقيقة إزاء سلبية هؤلاء الضحايا، هو إصرارهم على إخفاء الجرائم التي وقعوا ضحية لها، على الرغم من توصيات العديد من المنظمات في هذا الشأن ويكفي إقناعهم كي يحاولوا مقاومة ظاهرة الغش المعلوماتي، وتكمن أول مرحلة في هذا الشأن، في المعرفة الجيدة بهؤلاء مرتكبي أفعال الغش، والتقنيات التي يستعملونها، والقطاعات الأساسية التي يستهدفونها، ويبقى الكثير من جميع الحالات من أجل فهم ظاهرة الغش المعلوماتي وآلياتها، وهي مهمة على قدر من الصعوبة بالنظر إلى التقنية العالية للوسائل المستخدمة من أجل اقتراف فعل الغش وإلى تعقد التكنيك المعلوماتي ذاته.

---

(1) Y. Bismuth, art prec, p. 366..

الفصل الثالث: التقنيات المستخدمة لارتكاب الجريمة المعلوماتية

كثيراً ما يتواءم المجرمون والتقدم التقني، شأنهم في هذا المجال شأن المستخدمين الشرعيين للأجهزة المعلوماتية، ويظهر مرتكبو أفعال الغش كل أنواع الحيل والمكائد لخداع الحاسب الآلي، ومن ثم إسقاط حواجز الأمن سواء كانت مادية أو الكترونية.

وتعكس لنا الإحصائيات النادرة في مجال ظاهرة الغش المعلوماتي - حقيقة مؤلمة تكاد تكون أقرب إلى الخيال، وهي أن هذه الظاهرة المستخدمة للإجرام لن تتوقف عن الإزدياد، وتظل من جهة أخرى تفوق بعشرين مرة نظيرتها في مجال السطو المسلح.

وسوف نحاول في هذا الخصوص أن نحصي تقنيات الغش الأساسية المستخدمة، أو على الأقل تلك التي أمكن اكتشافها وأشار إليها المتخصصون، ونحن على ثقة تامة من أن هذه المحاولة ستكون محفوفة بالرقم الأسود الذي يسيطر على هذا المجال.

وإذا كان الحاسب الآلي هو رمز القوة وأداة السلطة، إلا أنه يسهل التعدي عليه دائماً عن طريق أحداث طبيعية أوأحداث من صنع الإنسان، وتلك الأحداث يمكن أن تدمره كلية أو بصفة جزئية، وعلى سبيل المثال يمكن لحريق أو فيضان أن يدمر المعلوماتية نهائيا، أو يجعلها غير قابلة للاستخدام المؤقت.

ويمكن لأي ارتفاع غير عادي في درجة الحرارة في صالة الحاسب الآلي أن يؤثر على أدائه الوظيفي أو يمحو بدون قيد أو شرط محتوى الشرائط

المغنطة، وهذا ما حدث عندما قامت شركة IBM بارسال بعض البرامج المعلوماتية إلى أفريقيا حيث تسببت عاصفة في نشاط الشرائط أثناء الرحلة.

ومن جهة أخرى، فقد يكون الحاسب الآلي محلا لتيارات أيديولوجية متباينة، لذا فليس من المستغرب أن يكون مستهدفا بواسطة أفعال تعدى معتمدة وعنيفة وأيضا، وقد تتبلور في صورة الاعتداءات باستخدام المواد المتفجرة أو أفعال التخريب.

ولا يستدعي هذا الإجرام العنيف أن نفرد له دراسة خاصة، حيث لايثير من الناحية القانونية أي مشاكل، ويمكن أن تطبق بسهولة النصوص الجنائية التقليدية الخاصة بانتهاك حرمة المسكن، أو الإتلاف والتخريب . .الخ.

وكما سبق الإشارة فإن مرتكبي أفعال الغش المعلوماتي. قد أثبتوا مهارة فائقة في اقتراف أفعالهم المعلوماتية غير المشروعة والتي تبدو حداثتها في ذاتية التقنيات والوسائل المستحدثة، ونقترح من أجل كشف النقاب عنها أن نعالج المسألة من خلال محورين :

المحور الأول : وفيه يلاحظ ارتكاب الجريمة المعلوماتية من خلال أداء الحاسب لوظائفه الطبيعية.

المحور الثاني : وفيه يتم ارتكاب الجريمة المعلوماتية من خلال التعدي على وظائف الحاسب الآلي.

المبحث الأول : الجرائم المرتكبة أثناء أداءالحاسب الآلي لوظائفه الطبيعية

لا تستلزم هذه الجرائم تدخلا لإتلاف الوظائف الطبيعية للحاسب الآلي. ولا تعديل على البيانات المعالجة، بل تقتصر على العكس وفي

الغالب الأعم ولوجا ماديا من جانب البعض في مركز المعالجة، وأداة الكترونية مصطنعة تسمح بالتقاط والتنصت عليه من بعد.

المطلب الأول: الالتقاط غير المشروع للمعلومات المعالجة بواسطة الحاسب الآلي

وكما سبق الاشارة، فإن التواجد في مركز المعالجة، وفي صالات الحاسبات الالية، هو أمر حتمي لارتكاب هذه الجرائم، ويتمثل الفعل غير المشروع في الإطلاع غير المصرح به بالمعلومات المختزنة في ذاكرات الحاسبات الآلية، وله صور عديدة :

١ ـ سرقة القائمة

وهي عملية مادية بحتة، يكتفي فيها السارق بسحب القائمة من الطابعة Imprimante

٢ ـ الاطلاع على المعلومات

أي الاطلاع على المعلومات التي تظهر على شاشة كاثوبدة +++ والمتصلة بالحاسب الآلي، ويمكن أن تعتبر هذه العملية من قبيل الالتقاط الذهني.

٣ ـ التنصت المجرد على المعومات

ويتم ذلك عن طريق وسيط، وهو عبارة عن مكبر الصوت الذي يلتقط المعلومات والبيانات المعالجة، ويعد هذا النوع من الالتقاط ـ طبقا لآراء الخبراء ـ أكثر الأفعال غير المشروعة ارتكابا وأسلهلها من حيث التنفيذ.

وتنشأ هذه الجريمة، إذا كان المستفيد من التنصت ليس لديه الحق في تلقي المعلومات المعالجة، أو إذا كان لديه الحق في استقبالها، ولكنه استخدمها في أغراض غير مسموح بها.

وفيما يتعلق بالفرض الأول، نستطيع أن نذكر على سبيل المثال، واقعة ولوج موظف سابق بأحد البنوك الفيدرالية الأمريكية في النظام المعلوماتي الخاص لهذا البنك باستخدام كلمة السر والتي حصل عليها من زميل سابق له، ونجح في التقاط المعلومات المالية المختزنة فيه، ونقلها إلى رئيسه الجديد في العمل كي يستفيد منها.

ونجد في بعض الفروض الأخرى، أن المستفيد من المعلومات قد تكون لديه الصفة اللازمة، أي الحق في الاطلاع عليها، ولكن يستغلها على نحو غير مشروع. وقد لاحظ ذلك رجال الشرطة والجمارك في سويسرا من خلال حركة الحسابات البنكية التي افتتحها بعض الفرنسيين خلسة، والتي تعكس الميل إلى التسويق الخفي لمثل هذه المعلومات عن طريق الممولين.

واكتفى طالب جامعي - في حالة أخرى من حالات التقاط المعلومات، بجمع مخلفات أحد البنوك، وحشد قدراً لا يأس به من المعلومات الخاصة بالمركز المالي لأحد الأحزاب السياسية. وقد تمكن طالب آخر من إعادة تكوين المعلومات الخاصة بطلبية بضاعة كبرة بواسطة حاسب آلي، واستولى على معدات توازي قيمتها مليون دولار من إحدى الشركات بولاية كاليفورنيا++ وقد تذرع الطالب المذكور بمقابلة المسئول عن المركز المعلوماتي، واستفاد من لحظة اغفال هذا الأخير، لكي يستولي على القوائم الموجودة بسلة الأوراق، وقد تمكن من بيع المعدات المختلسة بمعاونة الحاسب الآلي عن طريق وساطة شركة أنشئت خصيصاً لهذا الغرض.

المطلب الثاني: السطو المسلح الإلكتروني

أدى التطور المستمر لاستخدام المعلوماتية إلى التزايد الحتمي للمعالجات والتخزين، ومن ثم زيادة تدفق المعلومات في شكل ممغنط أو الكتروني بدلا من الشكل الكتابي.

كما ترتب على ظهور التقنيات المستحدثة، أي تقنيات بث المعلومات على شبه اتصالات بعدية والمعالجة عن بعد وإلى نشوء مخاطر جديدة نتيجة للإمكانات المستحدثة للولوج والاستفسار عن بعد من المراكز المعلوماتية، وتدور جميعها حول مشكلة تأمين الولوج المادي في المركز المعلوماتي، وتشكل عمليات البث أيضا نقطة ضعف هامة في النقاط المعلوماتي.

ويمكن أن نصادف المشاكل المرتبطة باستخدام أنظمة المعالجات عن بعد وشبكات البث في مراحل عديدة ومختلفة لاستعمال الأساليب الالكترونية، وفي الواقع، فإن المعلومات أثناء حركتها وبثها، تكون مهددة في كل لحظة بالالتقاط أو التسجيل غير المشروع.

١ ـ التقاط المعلومات المتواجدة ما بين الحاسب الآلي والنهاية الطرفية

يتم هذا الالتقاط عن طريق توصيل خطوط تحويلة، والتي ترسل إشارات الكترونية «ذبذبات الكترونية مكبرة» تمثل المعلومات المختلسة إلى النهاية الطرفية المتجسسة، أو عن طريق مرسل صغير يسمح بنقل المعلومات من بعد.

وعلى النقيض عندما تسلك المعلومات الطريق الجوي «كما في حالة البث عن طريق القمر الصناعي»، توضع هوائيات مطاردة بالقرب من الهوائيات الاحتياطية، والتي تسمح بالتقاط الإشعاعات واحتجاز مضمونها.

٢ ـ التوصيل المباشر على خط تليفوني

وقد سبق معرفة هذه التقنية في بعض المجالات، وتباشر عن طريق وضع مركز تنصت يسهل تسجيل كل الاتصالات، كما يمكن أن تؤدي هذه الوظيفة ميكروفات صغيرة.

٣ ـ التقاط الإشعاعات الصادرة عن الجهاز المعلوماتي

ويمكن عن طريق هذه التقنية إعادة تكوين خصائص المعلومات، التي تتحرك وتنتقل من خلال نظام معلوماتي، ويكفي لاتمام ذلك أن تسجل ثم تحل شفرة الاشعاعات الالكترو مغناطيسية المنبثة بواسطة أجهزة الكترونية.

وفي الحقيقة، تصدر بعض عناصر الأنظمة القوية ـ وعلى وجه الخصوص الطابعات السريعة أثناء تأدية وظيفتها إشعاعات الكترومغناطيسية وقد ثبت أنه بإمكان شاحنة صغيرة مجهزة تجهيزاً خاصاً وتقف بمحاذاة مبنى مكتظ بالحاسبات الآلية أن تلتقط وتسجل هذه الاشعاعات. ويمكن عن طريق جهاز لفك الرموز أن يطلب من طابعة متصلة بنظيرتها الموجودة في المركز المستهدف النسخ الحرفي لنفس هذه المعلومات. ويحضرنا في هذا الخصوص مثال شهير للسطو المسلح الالكتروني. وهو خاص باختلاس أموال عن طريق التقاط أمر بالتحويل مرسل من بنك إلى آخر وقد تمكن المختلس من تزييف الرسالة بالأمر بدفع نفس المبلغ لحساب فتح باسمه.

٤ ـ التدخل غير المشروع في نظام بواسطة طرفية بعدية

يمكن عن طريق تقنية التدخل في نظام معلوماتي من بعد، ثم يصبح بعد ذلك نسخ أو تدمير بعض المعلومات شيئاً سهلاً. ويكفي لبلوغ ذلك

الحصول على حساب آلي ميكروي ومودم + والتزود بكلمة أو مفتاح الشفرة المناسب.

بعد على ذاكرات الحاسبات الآلية بالخاصة بالشركة الدولية للخدمات المعلوماتية C.I.S.I وهذه هي إحدى الحالات النادرة التي كشف عنها في فرنسا.

وفي المقابل، تستلزم بعض أفعال الغش المعلوماتي التعدي على الوظيفة الطبيعية للحاسب الآلي، وقد تتحقق أفعال الغش هذه من جهة عن طريق التعدي على المعلومات، وقد تتحقق من جهة أخرى عن طريق التعدي على البرامج المعلوماتية.

المبحث الثاني: الجرائم التي تستلزم التعدي على الوظائف الطبيعية للحاسب الآلي

أبرز ارتكاب مجموعة أخرى من الجرائم المعلوماتية، السمة العالية لتقنية أفعال تعدي المحتالين، والتي تتجسم في صورة المعالجة غير المشروعة سواء للمعلومات أو البرامج ذاتها.

المطلب الأول: التعدي على المعلومات

يعد التلاعب في المعلومات - وفقاً لآراء الخبراء - من أكثر أفعال الغش ارتكاباً في أوربا، ويتم هذا التلاعب إما عن طريق إدخال معلومات مصطنعة أو إتلاف المعلومات الموجودة بالآلة.

أولاً: إدخال معلومات مصطنعة

يعد المسئول عن القسم المعلوماتي، والذي يستند إليه على وجه

الخصوص وظيفة المحاسبة والمعاملات المالية، في أفضل وضع يؤهله لارتكاب هذا النمط من التلاعب غير المشروع.

ويبدو أن الغش في الدفع الأكثر تكرارا سهولة في التنفيذ لا سيما في وسط منشأة تملك قدراً كبيراً من النقود والذي يتباين تبعاً للظروف.

١ ـ ضم مستخدمين غير موجودين بالفعل

وينطبق ذلك على وجه الخصوص بالنسبة لمنشأة تضم العديد من الفروع والتي تغير عدد مستخدميها وفقاً للظروف الاقتصادية وقائمة الطلبات. حيث يقدم مدير أحد هذه الفروع معلومات وهمية إلى الإدارة المركزية خاصة باستئجار مستخدمين مؤقتين، ويكفي بالنسبة له، وفي نهاية كل تعد، أن يستلم الشيكات النقدية الخاصة بالمستخدمين المؤقتين المزعومين. وقد وقعت شركة الشيكات النقدية الخاصة بالمستخدمين المؤقتين المزعومين

وقد وقعت شركة ASSE-DIC ضحية لمثل هذه الأفعال غير المشروعة. وبالمثل أيضاً فقد استطاع أحد المسئولين عن القسم المعلوماتي بإحدى الشركات الفرنسية اختلاس أكثر من مليون فرنك فرنسي وقام بإيداع هذا المبلغ في حسابه الشخصي وحساب شركائه في العمل الإجرامي. ولكي يحقق ذلك أعاد ملفات المستخدمين السابقين والذين لهم حقوق مالية وقام بتحويلها الى حسابه وحسابات أخرى تم افتتاحها خصيصا لهذا الغرض عن طريق شركاء. وبعد ارتكاب الجريمة قام بإصلاح الموقف السابق بمحو كل آثار فعل الغش المعلوماتي. ومن المستحيل تنفيذ مثل هذه العملية إلا باستخدام حاسب آلي والذي يمكن أن نأمر بتغاضي عن بعض المعاملات المالية.

٢ ـ الإبقاء على مستخدمين تركوا الوظيفة بالفعل

ويتلخص هذا النمط من أفعال الغش المعلوماتي، في أن المبرمج المسئول عن الإدارة المالية المعلوماتية بدلا من أن يحفظ ملفات الأشخاص الذين تركوا العمل بالمنشأة، فإنه يبقى هؤلاء الملفات على قيد الحياة ويجعلها تدر دخلا مع نهاية كل شهر

٣ ـ اختلاس النقود

قامت شرطة مارسيليا الفرنسية بالقبض على مستخدم يعمل لدى فرع مصرفي تابع لبنك INDO-SUEZ ووجهت إليه تهمة اختلاس ٧ ملايين فرنك فرنسي.

وقد تمكن من عمل تحويلات لنقود وهمية مستخدما في ذلك الحاسب الآلي الخاص بالبنك، والمبالغ الدائنة ولو أنها لم ترد في الخزينة إلا أنها قد سجلت في ذاكرة الحاسب الآلي قبل أن تنقل بواسطة محررات مصطنعة من حساب فتح باسمه في سويسرا.

وفي الواقع، بإمكان أي شخص يشغل مركزا على قدر من الأهمية في أحد المنشآت أو البنك، ولديه الكفاءة الفنية اللازمة لاستخدام الحاسب الآلي. أن يغترف من هذا الأخير ما يشاء من المعلومات التي يرغب فيها، وليس بامكان الحاسب الآلي أن يراقب مدى مشروعية هذا العمل.

وهناك أيضاً قضية شهيرة تم كشفها في إسرائيل في فبراير ١٩٨١م وتتلخص وقائعها في أن شخصا يدعى Vladimir Loriblitt وهو مهاجر روسي عمل كمبرمج في وزارة المالية، وكان مولعا باصطناع الشركات الوهمية وقد أدخل في الحاسب الآلي فواتير وهمية لا حصر لها. وقد

سمح له ذلك أن يحول إلى هذه الشركات الشيكات العديدة والمسددة من T.V.A.

ثانياً : إتلاف المعلومات

يمكن للمسئولين عن حفظ المعلومات ـ وبمنتهى البساطة ـ أن يغيروا ويتلفوا المعلومات بحفظها داخل جهاز الحاسب الآلي .

ومن الأمور السهلة في الواقع استبدال رقم حساب بآخر ، أو إحلال بطاقة محل أخرى ، وهذا النوع من الجرائم على قدر كبير من الخطورة ، لأنه في حالة نجاح التزوير ، يمكن للجريمة أن تستمر لفترة من الزمن حتى يتم كشف الفعل غير المشروع . وهناك مجموعة من المستخدمين الإداريين على سبيل المثال استطاعوا خلال سنوات عديدة أن يضاعفوا من رواتبهم عن طريق الحاسب الآلي ، حتى لحظة الكشف عن هذا العمل الآثم بمحض الصدفة .

وهناك البعض الآخر الذي تقاضى ساعات إضافية لم يتم تنفيذها على الإطلاق وذلك عن طريق استبدال قوائم الحسابات بساعات العمل .

وقد أمكن تقديم بعض مرتكبي جرائم التزوير في المعلومات للمحاكمة ، وهذا ما حدث بألمانيا الشرقية ، حيث قام مستخدم بمكتب القوى العاملة ، كان مكلفا بتوزيع الإعانات العائلية ، بتحويل مبلغ وقدره ٥٠٠ , ٠٠٠ مارك لحسابه في شكل مرتبات وقد أزال من المنفذ الخاص بمراقبة الحاسب الآلي الرقم الأول للمبالغ المحولة وقد حكم عليه بالسجن لمدة ثلاث سنوات .

وقد لجأ بعض مرتكبي أفعال الغش المعلوماتي الأكثر مهارة إلى الهجوم

المباشر على المعلومات المحمولة بواسطة شبكات الاتصال البعدية وهم شديدو الولع بالتقاط أذونات التحويل عن طريق وسائل الكترونية مصطنعة وتزويرها بالأمر بدفع نفس المبلغ ولكن لحساب آخر، ويتم اتلاف المعلومات أو تعديلها بوسائل متعددة منها :

١ ـ ممارسة Balff ٥٠ ـ تتمثل هذه الممارسة في استخدام الحاسب الآلي من أجل طبع فواتير مصطنعة أو فواتير ذات قيمة كبيرة ويقوم العملاء بتسديدها منخدعين في الثقة التامة التي يستلهمونها من استخدام الحاسب الآلي، والقليل من هؤلاء الذين يبدون اعتراضهم يتلقون خطابا تفسيريا مذيلا بصيغة صارت تقليدية «تقبلوا عذرنا، قد أخطأ حاسبنا الآلي» وهكذا يستخدم الحاسب الآلي والمتهم بسوء الإدارة ككبش فداء.

٢ ـ أخفقت عملية نصب قدرت بحوالي ٢١ مليون فرنك فرنسي بسبب خطأ معلوماتي مبتدأ، وتتخلص وقائع هذه الدعوى أنه في ٢٩ فبراير ١٩٨١م وصل إلى أحد فروع الشركة العامة شريط ممغنط قادم من شركة Isover St Gobain وقد إحتوى هذا الشريط على ١٣٩ إذناً بالدفع، عند معالجته بالقسم المعلوماتي للبنك، فقد تم رفضه بواسطة الحاسب الآلي نتيجة لعيب جسيم يتعلق بطول تسجيل الشريط، وقد ألقي القبض على مرتكب هذه المحاولة للنصب.

وكان بالإمكان ـ وفقاً لآراء الخبراء ـ أن يكتب لهذه المحاولة النجاح إذا توافر لدى المزيف المعرفة التقنية اللازمة في المجال المعلوماتي.

٣ ـ محو المعلومات : تمكن شخصان من اختلاس ٦١,٠٠٠ دولار، وهي عبارة عن مبالغ مدفوعة مرسلة من شركات التأمين إلى أحد المراكز الجامعية، ولكي يؤدي كل من المحللين عملهما الآثم على خير وجه،

فقد قاما بمحو كل الحسابات القائمة في تسجيلات الحاسب الآلي الخاص بالمركز وجعلها غير قابلة للتحصيل.

وبالإمكان أيضا أن تكون البيانات المعلوماتية فقط محلا للمحو الانتقائي، ولكن أيضا للالغاء بلا قيد أو شرط.

وهكذا تم الكشف في مدينة دالاس الأمريكية أن أربعة من مستخدمي بلدتها، كانوا قد استبعدوا ٢٧١ مخالفة من سجلات المدينة مقابل تقاضي نسبة مئوية محددة بلغ مجموعها ١٦,٣٠٠ دولار

٤ ـ التلاعب في المعلومات من بعد: يمكن أن تنفذ هذه في حين يوجد مرتكبها على بعد عدة كيلومترات من مكان الاقتراب النهائي للجريمة.

ويستطيع مرتكب فعل الغش المعلوماتي إذا ما تزود ـ كما سبق الإشارة ـ بكلمة السر أو مفتاح الشفرة وأداة ربط، نقول يستطيع أن يغير من أي مسافة محتوى الذاكرات، وأن يستبدل أرقام الحسابات إحداها بالأخرى. ويروي في هذا المجال قصة الطالب الأمريكي، والذي بعد أن تدخل تدخلا غير مشروع في أحد النظم المعلوماتية، أصبح مالكا له لفترة من الزمن، بعد أن قام بتغيير مفتاح الشفرة. وقد ترتب على ذلك أن رفض هذا النظام أن يمد أصحابه ومستخدميه الشرعيين بالخدمات المعلوماتية لبضعة ساعات، وهذا يشير إلى مدى جسامة الاعتداء بالوسائل المعلوماتية.

وسوف نحاول بعد هذا الحصر لبعض أفعال التعدي على المعلومات، أن نحصي بعض أفعال تعد أخرى أكثر جسامة وأكثر تزييفا، أي أفعال الاعتداء على الكيانات المنطقية والبرامج التي تتحكم في أداء النظام المعلوماتي لوظائفه.

المطلب الثاني: التعدي على برامج الحاسب الآلي

يستلزم هذا النمط من الجرائم - وهو جرائم المتخصصين - معرفة فنية كبيرة في مجال البرمجة . وتنفيذه - وإن كان من الصعوبة بمكان إلا أنه يمكن أن يتحقق في مراحل مختلفة من صنع برنامج التشغيل أو التطبيق أو في لحظة صيانتها أو تحديثها .

أولاً : التعديل في برنامج تطبيقي

يمثل هذا النوع من التعديل نسبة تقدر بحوالي ١٥٪ من مجموع حالات الغش المعلوماتي المحصورة . واختلاس النقود في معظم هذه الحالات كان الهدف المبتغى . ويذكر في هذا المجال واقعة مبرمج كان يعمل بأحد البنوك وقام بوسيلته الخاصة بتعديل برنامج إدارة الحسابات ، وبحيث يضيف ١٠ سنتات لمصاريف إدارة الحسابات الداخلية على كل عشرة دولارات ، دولار واحد على الحسابات التي تتعدى ١٠ دولارات . وتم قيد المصاريف الزائدة في حساب خاص فتحه باسم مستعار ، وهكذا حصل على عدة مئات من الدولارات كل شهر ، وكان بالإمكان أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافىء أول وآخر عميل له وفقا للترتيب الأبجدي ، وحينئذ اكتشف عدم وجود ما يدعى .

وهناك مثال آخر لمستخدم أمريكي يدعى E.Royce كان يعمل بإدارة ائتمان منشأة تجارية كبرى «الإتجار بالجملة للفواكه والخضروات» لجأ إلى هذه الوسيلة للغش والتي يطلق عليها Salami وتتمثل في برمجة الحاسب الآلي بحيث يستقطع بعض السنتيمات من الايداعات الدورية «وعلى سبيل المثال جبر الكسور عن طريق الخطأ» وتحويلها إلى حسابات خاصة .

وهذه العملية مجزأة جداً، وهكذا استطاع مستخدم بإحدى شركات التأمين برمجة الحاسب الآلي وبحيث يستقطع كسور السنتيمات من كل عمليات الشركة، ويتم تحويلها إلى حسابه السري.

وقد تم برمجة الحاسب الآلي ببراعة، لكي يجبر في كل مرة الأرقام وتبقى الميزانيات متعادلة، ولا يشوبها أي شائبة.

وقد أطلق على هذه التقنية مصطلح Perruque بسبب استقطاع سنتيم بسنتيم، على نمط الحلاق الذي ينجز عمله شعره بشعره، وتنطبق أيضا في البنوك والتي تمنح فوائد للحسابات الجارية.

وقد يصل الأمر أحيانا بالمبرمجين من ذوي النوايا السيئة إلى زرع برنامج فرعي غير مسموح به في البرنامج الأصلي، وهو معروف لهم فقط ويسمح لهم بالولوج غير المشروع في موردات «وهي عبارة عن العناصر الضرورية لأي نظام معلوماتي» الحاسب الآلي.

ويمن دفن هذا البرنامج الصغير السري وبمهارة بين آلاف التعليمات التي تكون برنامجاً معلوماتياً.

وقد وجد أن أكثر وحدات الضبط دقة لا تستطيع كشف التعليمة المسلوبة، وهذا لا يحدث إلا بمحض الصدفة. ويحضرنا في هذا المقام مثال خاص بمنشأة للكليات المنطقية أضاف مبرمجها إلى البرنامج المعلوماتي الخاص بإدارة الحسابات أن يتجاهل كل عمليات السحب التي تتم بمعرفة المبرمج سواء عن طريق بطاقات أو شيكات حسابية. وقد تحمل البنك هذه المسحوبات من باب ميزانية الإدارة.

واكتشفت عملية الغش المفهرسة تحت اسم «حصان طروادة» بمحض

الصدفة عندما حدث عطل بأحد النظم المعلوماتية، مما استلزم معالجة يدوية لكل الحسابات.

وهكذا برمج مستخدم بقسم الصيانة المعلوماتية تحويل النقود عن طريق تعليمات إضافية في البرنامج. ولم يتم هذا التحويل بالفعل إلا بعد مضي ثلاثة أشهر من رحيله من البنك. وقد استخدمت هذه التقنية في ألمانيا «مثال سبق ذكره» حيث تم تدمير الذاكرة المعلوماتية في تاريخ محدد بمضي عشرة أشهر من رحيل المحلل المعلوماتي.

وهناك أيضاً التقنية المعروفة تحت مصطلح Bombe logique وهي قريبة الشبه من القنبلة الزمنية، والتي تسمح بتحريك أحداث مستقبلية في تاريخ محدد أو طبقا لوقوع أحداث معينة.

وقد استوحى Thery Breton هذه التقنية وشيد على أساسها قصة واقعية، أطلق عليها الحرب الناعمة. وتدور أحداث هذه القصة حول مهندس شاب، أسس في الولايات المتحدة نموذجا لشركة خدمات معلوماتية، وغايتها وصف «الحرب الناعمة» التي تدور أحداثها بين الولايات المتحدة والاتحاد السوفيتي «سابقا».

وقد وافق الجانب الأمريكي على بيع كيان منطقي معقد جدا للدول الشيوعية، ويستخدم في المراكز الحسابية، ولكن قبل أن تتم هذه الصفقة فقد قامت الإدارات الأمريكية المختصة بإدخال تعليمات بالتوقف في هذا الكيان المنطقي، وهي تعليمات تسمح في لحظة معينة بتعطيل البرنامج وأصابت أيضا ادارة مركز الحسابات القائم في الدول الشيوعية بالشلل.

وقد ترتب على ذلك خسائر جسيمة، ويمكننا ملاحظة أن الأضرار الناشئة عن هذه التقنية من تقنيات الغش المعلوماتي آخذة في الازدياد بشكل غير مألوف.

ثانياً : تعديل برنامج التشغيل

يسمح برنامج التشغيل بتنظيم وتزامن وضبط توالي التعليمات والوظائف الخاصة بالحاسب الآلي، والتقنية الأخيرة، والتي تتخذ من برنامج التشغيل هدفا لها، وهي ما يطلق عيها المصيدة.

أ ـ المداخل المميزة

يمكن أن يحتوي أي برنامج في نسخته الأولى على أخطاء وعيوب، وقد لايكتشف البعض منها إلا عند استخدامه، ويتوقع المبرمجون النابهون إمكانية الولوج المباشر في البرامج الأساسية لتصحيحها.

ويمكنهم عن طريق المداخل المميزة ـ والتي هي في حقيقتها عبارة عن ممرات خالية متروكة في البرنامج ـ أحداث تعديلات في الشفرة والمنافذ الوسيطة وتستبعد بالطبع هذه المنافذ عند التصحيح النهائي للبرنامج المذكور وقد يصل الأمر أحيانا ببعض المبرمجين من ذوي النوايا السيئة، والذين لهم دراية بأهمية السلاح التقني الموجود بين أيديهم بأن يتغاضوا عن استبعاد هذه المداخل المميزة ولايتبهوا اليها أي شخص، ولكونهم هم المؤتمنين فقط على السر، فيمكنهم في لحظة معينة أن يستخدموا هذه المصيدة، وفقاً لهواهم، ويستمرون إذن في استغلال البرنامج المعيب من الناحية الفنية.

ومن الأهمية بمكان أن نشير إلى أنه بالإمكان، وعن طريق هذه المداخل المميزة الولوج في كل المعلومات التي تحتويها ذاكرات الحاسبات الآلية، ومن ثم التوصل الى الشفرات والتعليمات.

وباختصار يمكن عن طريق هذه الوسيلة، أن يصبح مرتكب فعل الغش، هو سيد النظام المعلوماتي مع ما يترتب على هذا الموقف من نتائج

إيجابية بالنسبة له، ونتائج سلبية جسيمة بالنسبة لصاحب أو المستخدم الأصلي للحاسب الآلي المسلوب.

٢ ـ اصطناع برنامج

يقصد الخبراء المعلوماتيون بلفظي «صنيع وتشكيل» استخدام الحاسب الآلي من أجل التخطيط للجريمة ومراقبتها وتنفيذها، أي اصطناع برنامج كامل ومخصص فقط لارتكاب فعل الغش المعلوماتي.

والمثال الذي يساق عادة بمناسبة هذا النمط من الغش، هو ذلك الخاص بشركة تأمين بلوس أنجلس، والتي اختلقت بفضل حاسبها الآلي ومعاونة مبرمجها عددا وهميا من المؤمن عليهم بلغ اجماليه ٦٤,٠٠٠ وثيقة تأمين.

وقد تقاضت الشركة المذكورة من اتحاد شركات التأمين عمولات نظير ٦٤,٠٠٠ وثيقة، واقتصر دورها فقط على إدارة لحسابات وإمعانا في التضليل، وبغرض إعطاء العقود الوهمية مظهراً مشابها للحق، قامت الشركة المذكورة بتنشيط الملفات المختلفة عن طريق تغيير الموطن والوظيفة وبعض الإقرارات الخاصة.

وفي النهاية يشهد هذا النوع من التعدي سواء على المعلومات أو البرامج المعلوماتية توسعاً ملحوظاً، في حين يقف في مواجهته المسئولون عن الأنظمة والمراكز المعلوماتية مكتوفي الأيدي.

المطلب الثالث: سرقة وقت الآلة

توجد مجموعة أخرى من الجرائم المعلوماتية قلما يعاقب مرتكبها وكثيراً جداً ما يتسامح ضحاياها بشأنها. ونعني بذلك الاستخدام غير المشروع للحاسب الآلي. أي استخدام وقت الحاسب الآلي أو وقت الآلة

من أجل أغراض شخصية، وقد يحدث عملاً، وبدلاً من الإبقاء على استخدام الجهاز المعلوماتي والموجود مكان العمل لأغراض مهنية بحتة ومسموح بها، فقد يتم الاستيلاء على وقت هذا الجهاز بمعرفة بعض المستخدمين غير الأمناء من أجل انجاز أعمال خاصة وبدون علم الحائز الشرعي للنظام المعلوماتي.

وجريمة سرقة وقت الآلة من الجرائم الشائعة في العديد من مراكز الأبحاث في فرنسا فمن السهولة بمكان أن ينتقل باحث من جل توفير نفقات معمله إلى مركز آخر وأن يستعير كلمة السر أو شفرة الوصل للولوج في بنك المعلومات الخاص به.

ويعد هذا الوقت للحاسب الآلي من الأمور المكلفة جداً، وقد يتسبب محاسب غير أمين في إحداث خسائر لمنشأة نتيجة لاقتراقه هذه الجريمة، تفوق بأضعاف أجور المستخدمين بها.

ويمكن أن نذكر في هذا الخصوص واقعة اثنين من مستخدمي شركة غاز بريطانية، قاما عن طريق اعلانات صغيرة ببيع رسومات صممت بواسطة النظام المعلوماتي الخاص بهذه الشركة. وهذا يساوي من الناحية العملية «العمل في الظلام» على حاسب آلي مملوك لرب العمل ولكن بدون علمه.

وهناك أيضا المثال الخاص بـ ٢٠٠ مستخدم الذين قاموا باستخدام الحاسب الآلي الخاص بمركز تصنيع وحماية الصواريخ النووية من أجل تخزين ألعاب اليانصيب والخطابات الشخصية.